УДК 343.985:004(045)

Верченко В.П.,
старший викладач,
Юридичний інститут,
Національний авіаційний університет, м. Київ

ТИПОВІ ПОМИЛКИ, ЯКІ ВЧИНЮЮТЬСЯ ПРИ ПРОВЕДЕННІ СЛІДЧИХ ДІЙ У ВІДНОШЕННІ ДО КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ АБО САМИХ КОМП'ЮТЕРІВ

Співробітниками правоохоронних органів допускаються певні помилки при розслідуванні злочинів, пов'язаних з комп'ютерним забезпеченням та захистом інформації, встановленої на комп'ютери їх безпосередніми користувачами. Як відомо виявлення, огляд і вилучення комп'ютерної інформації, як і самих комп'ютерів у ході слідчих дій можуть здійснюватися не тільки при слідчому огляді, але і при проведенні інших слідчих дій: обшуку, виїмки, відтворенні обстановки та обставин події.

Розглянемо деякі типові помилки, які часто вчинюються при проведенні слідчих дій у відношенні до комп'ютерної інформації або самих комп'ютерів. Можна виділити деякі правила роботи з комп'ютерами, вилученими при розслідуванні злочинів у сфері комп'ютерної інформації, а також запропонувати загальні рекомендації, що можуть бути корисні при обробці комп'ютерних доказів, працюючи в операційних системах DOS чи Windows.

Помилка 1. Помилкова робота з комп'ютером.

Перше та основне правило, що неухильно повинне виконуватись, полягає в наступному: ніколи і ні при яких умовах не працювати на вилученому комп'ютері. Це правило припускає, що вилучений комп'ютер-насамперед об'єкт дослідження фахівців. Тому його бажано навіть не включати до передачі експертам, оскільки категорично заборонено використовувати будь-які програми на вилученому комп'ютері без вживання необхідних заходів безпеки (наприклад, захисту від модифікації або створення резервної копії). Якщо на комп'ютері встановлена система захисту на вході в нього (наприклад - пароль), то його включення може викликати знищення інформації, що знаходиться на жорсткому диску. Не допускається завантаження такого комп'ютера з використанням його власної операційної системи.

Така міра пояснюється досить просто: злочинцю не складає особливої труднощі установити на своєму комп'ютері програму для знищення інформації на жорсткому чи гнучкому магнітному диску, записавши таки "пастки" через модифікацію операційної системи. Наприклад, проста команда DIR, яка використовується для відображення каталогу диска, може легко бути змінена, щоб відформатувати жорсткий диск.

Після того як дані і сама руйнуюча програма, знищені, ніхто не зможе вірогідно сказати, чи був "підозрюваний" комп'ютер спеціально оснащений такими програмами, чи це результат недбалості при дослідженні комп'ютерних доказів?

Помилка 2. Допуск до комп'ютеру власника (користувача) комп'ютера.

Серйозною помилкою є допуск до досліджуваного комп'ютера власника для допомоги при його експлуатації. У багатьох зарубіжних літературних джерелах описуються випадки, коли підозрюваному на допиті пов'язаному з комп'ютерними доказами, було надано доступ до вилученого комп'ютера. Пізніше вони розповідали своїм знайомим, як шифрували файли "прямо під носом у поліцейських", а ті при цьому навіть не здогадувалися. Враховуючи такі наслідки, дуже швидко комп'ютерні фахівці стали робити резервні копії комп'ютерної інформації перш, ніж надавати доступ до них.

Інша проблема пов'язана з можливістю спростувати у суді ідентичність пред'явленого у процесі програмного забезпечення тому, що знаходилося в даному комп'ютері на момент вилучення. Щоб уникнути таких ситуацій, комп'ютер треба не включаючи опечатати у присутності понятих. Якщо ж співробітник правоохоронних органів приймає рішення оглянути комп'ютер на місці, перше, що варто зробити це зняти копію з жорсткого магнітного диску і будь-якої дискети, що буде вилучатися як речовинний доказ. Це означає, що до проведення будь-яких операцій з комп'ютером необхідно зафіксувати його стан на момент проведення слідчих дій.

Помилка 3. Відсутність перевірки комп'ютера на наявність вірусів і програмних закладок.

Для перевірки комп'ютера на наявність вірусів і програмних закладок, необхідно завантаження комп'ютера не з операційною системи яка знаходиться на ньому, а з своєї заздалегідь підготовленої дискети, або з стендового жорсткого диску. Перевірці підлягають усі носії інформації – дискети, жорсткий диск та інші носії. Цю роботу варто робити залученому для участі в слідчих діях фахівцю, за допомогою спеціального програмного забезпечення.

Розглянутий перелік не охоплює всіх помилок, що виникають у процесі вилучення і дослідження комп'ютерної інформації. Цьому легко знайти пояснення: відсутність достатнього досвіду в подібних справах у нашій країні. У той же час у країнах Західної Європи і США є вже досить багатий досвід щодо розслідування складних комп'ютерних злочинів. Варто більш ретельно його вивчати, що дозволить уникнути багатьох помилок.

Як висновок, треба підкреслити, що будь які дії, пов'язані з розслідуванням злочинів у сфері використання комп'ютерних технологій, доцільно з самого початку залучення фахівця у галузі інформаційних технологій. До початку слідчих дій необхідно також мати певну інформацію щодо: марки, моделі комп'ютеру, операційної системи, периферійних пристроїв, засобів зв'язку та будь-які інші відомості про систему, котра є об'єктом розслідування.

Широке впровадження комп'ютерних технологій вимагає також певних змін у кримінально-процесуальних нормах, що регламентують процедури в частині використання нових джерел доказів.